ISSN Number: 2454-2024(Online)

International Journal of Technical Research & Science

CYBER ETHICS: AN IMPORTANT CONCEPT TO BECOME A RESPONSIBLE CYBER CITIZEN

Sourajit Kumar Banerjee[1], Arti Vaish[2]

E-Mail Id: sourajit.banerjee123@gmail.com, artivaish@sushantuniversity.edu.in

[1] School of Health Sciences, Sushant University, Gurgaon, Haryana, India

[2]School of Engineering and Technology, Sushant University, Gurgaon, Haryana, India

Abstract- In this digital era with more and more advancements there has been an increase in cyber security related issues. To address such things cyber ethics related awareness among common people is of utmost importance. While using cyber space we need to be ethically correct. It's our responsibility to be a good and morally strong cyber citizen. The concept of cyber ethics deals with various code of ethics. There is a great need for cyber ethics as various cyber related issues are increasing like spying, frauds, exploitative conduct. Preventive measures to deal with cyber crime related issues should be known by all. Some awareness programs should be conducted regarding various cyber ethics and cyber crime. Everyone must understand their responsibilities for conducting themselves online. An important component of that is Cyber Ethics. We all should implement cyber ethics to be a good "cyber citizens".

Index Terms: Cyber ethics, Cyber crime, Cyber space, Cyber attack, Cyber security.

1. INTRODUCTION

It is very important to know about the term Cyber ethics before moving further into our main topic. It is basically internet ethics, which involves studies related to moral dilemmas and ethical questions that are created by the growing digital technologies and also is a branch of applied ethics. Increased internet usage has lead to conflicts over security, accuracy, censorship, filtering, privacy, property, accessibility, and others have arisen [1-3].

For a long time, different legislatures have established guidelines while associations have characterized strategies about digital morals [4]. While laws are basically characterized inside the limits of a country state as the administrative body, ethicists look for more general reason for moral great and equity. Specifically, numerous digital ethicists carry on their talks inside multi-social conditions, without falling into extremist social relativism. Digital morals are the logical investigation of morals relating to Personal Computers (PCs), incorporating client conduct and what PCs are customized to do, and how this influences people and society. PC morals basically shield people online from predation: they forestall the break of security, distinguish robbery, impedance with work, and unlawful utilization of restrictive programming, among different occasions [5].

Rather than direct utilization of customary moral speculations like utilitarianism, deontological (morals of obligation), and uprightness morals, ethicists frequently endeavor to track down solid moral thinking as contextualized talk.

- The most effective method to ensure yourself against cybercrime are:
- Keep your product refreshed.
- Manage your online media settings.
- Strengthen your home organization.
- Talk to your kids about the web.
- Using proper security Protocols.
- Use solid passwords.
- Keep cutting-edge on significant security breaks.

Five arrangements of digital morals are: Your digital information ought not be utilized to take different people groups assets, Never utilize different people groups assets without their assent ,Your PC or framework ought not

be utilized to hurt others , One ought not utilize or duplicate programming projects for which you have not paid [6].

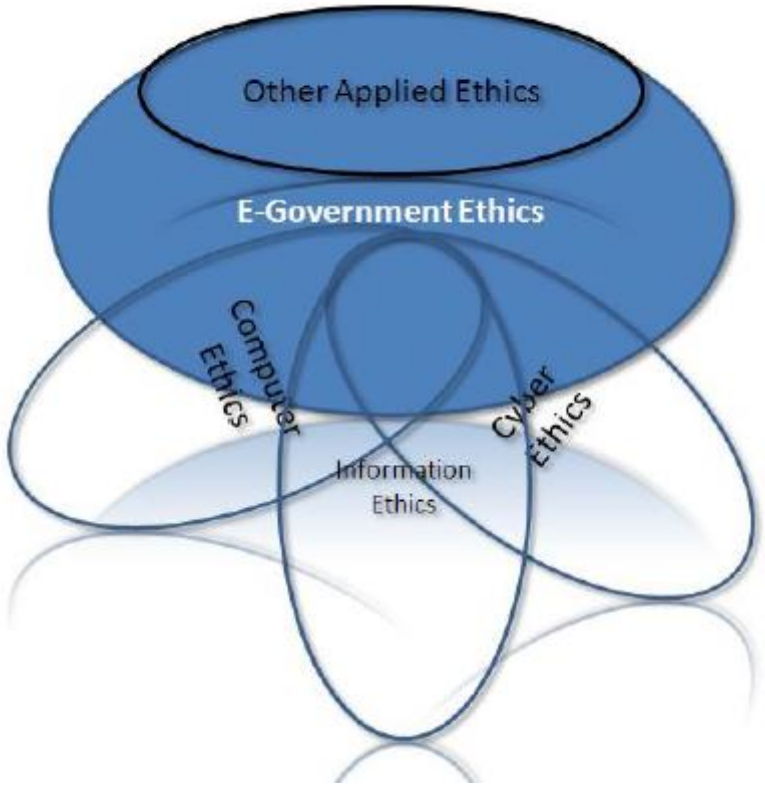

Fig. 1.1 Different Ethics Position

2. THE CONCEPT OF CYBER ETHICS

Data Technology administrators are needed to build up a bunch of moral principles normal to their association. There are numerous instances of moral code as of now distributed that can be custom-made to fit any association [7-9]. Code of morals is an instrument that builds up a typical moral structure for a huge gathering of individuals. Four notable instances of Code of Ethics for IT experts are recorded underneath-

2.1 Code of Ethics (ISC)

(ISC) an association focused on accreditation of PC security proficient has additionally characterized its own Code of Ethics for the most part as:

- Discourage perilous practices, and save and reinforce the uprightness of public frameworks.
- Observe and keep all agreements, communicated or suggested, and offer reasonable guidance.
- Discourage perilous practices, and save and reinforce the uprightness of public frameworks.
- Observe and keep all agreements, communicated or suggested, and offer reasonable guidance.
- Avoid any irreconcilable circumstance, regard the trust that others put in you, and take on just those positions you are able to perform.
- Stay current on abilities, and don't become engaged with exercises that could harm the standing of other security experts.
- Act sincerely, evenhandedly, mindfully, and lawfully, and securing the ward.
- Work tirelessly and offer able types of assistance and advance the security calling.
- Encourage the development of examination educate, coach, and worth the affirmation.

2.2 The Code of Fair Information Practices

The Code of Fair Information Practices depends on five standards laying out the necessities for records keeping frameworks. This necessity was executed in 1973 by the U.S. Division of Health, Education and Welfare.

- There should be a way for an individual to address or correct a record of recognizable data about the individual.
- Any association making, keeping up with, utilizing, or scattering records of recognizable individual information should guarantee the dependability of the information for their planned use and should avoid potential risk to forestall abuses of the information.
- There should be no close to home information record-keeping quiet.
- There should be a way for an individual to discover what data about the individual is in a record and how it is utilized.
- There should be a way for an individual to forestall data about the individual that was gotten for one reason from being utilized or made accessible for different purposes without the individual's assent.

2.3 RFC 1087

In January 1989, the Internet Architecture Board (IAB) in RFC 1087 characterizes an action as untrustworthy and inadmissible if it:

- Wastes assets (individuals, limit, PC) through such activities.
- Destroys the honesty of PC based data.
- Compromises the protection of clients.
- Seeks to acquire unapproved admittance to the assets of the Internet.
- Disrupts the planned utilization of the Internet.

2.4 Ten Commandments of Computer Ethics

The moral qualities as characterized in 1992 by the Computer Ethics Institute; a philanthropic association whose mission is to propel innovation by moral means, records these guidelines as a manual for PC morals:

- We shall not utilize a PC to bear bogus observer.
- We shall not duplicate or utilize restrictive programming for which you have not paid.
- We shall not utilize others' PC assets without approval or appropriate pay.
- We shall not proper others' scholarly yield.
- We shall ponder the social results of the program you are composing or the framework you are planning.
- We shall consistently utilize a PC in manners that guarantee thought and regard for your kindred people.
- We shall not utilize a PC to hurt others.
- We shall not meddle with others' PC work.
- We shall not nose about in others' PC documents.
- We shall not utilize a PC to take.

3. NEED FOR CYBER ETHICS

In current occasions with worries of protection, spying, hacking and so forth where no administration has control on the internet, a global body is must dependent on agreement. This body should chip away at a digital moral code or set of rules that would possibly be fit for managing people groups conduct on the web. Some issues where cyber ethics can play an important role are:

Spying: Actions, for example, states or enterprises keeping an eye on people, people keeping an eye on legislatures or partnerships, etc, raise the need of digital moral code. A digital moral code would illuminate residents regarding what is fortunate or unfortunate for them and will considered government responsible for untrustworthy activities [10].

3.1 Frauds

Fraud and pantomime is a portion of the vindictive exercises that happen because of the immediate or backhanded maltreatment of private data. Data fraud is rising quickly. Openly available reports web search tools and information bases are the principle offenders adding to the ascent of cybercrime. Moral business practice ensures the protection of their clients by getting data which might add to the deficiency of mystery, obscurity, and isolation.

3.2 Digital rights management (DRM)

Blind creation of book recordings of PDFs, permitting individuals to copy music they have really purchased to CD or to move it to another PC and so forth are viewed as infringement of the freedoms of the licensed innovation holders, making the way for uncompensated utilization of protected media. Another moral issue concerning DRMs includes the manner in which these frameworks could sabotage the reasonable use arrangements of the intellectual property laws. The explanation is that these permit content suppliers to pick who can view or pay attention to their materials making the oppression certain gatherings conceivable [11-14].

3.3 Increasing Cybercrime

Cyber-wrongdoing, hacking into people groups ledgers and taking their cash, or duping individuals in a bunch of ways is becoming pattern now. This expanding pattern of digital wrongdoing request need of legitimate arrangement of codes and rules.

3.4 Increasing exploitative conduct

There are numerous sorts of morally or ethically reckless conduct, in the space opened up by the web from activities including people groups monetary status, through disdain discourse or composing in regards to sexual orientation, race, culture, and a large group of other ethically questionable [15].

3.5 Threat to protection

Over 100 years after the fact, the web and expansion of private information through states and online business is a region which requires a new round of moral discussion including a people security. Protection from a moral and moral perspective ought to be integral to nobility and distinction and personhood. One must take the necessary steps to get all the protection. The hardship of protection can even imperil people's wellbeing. People give up private data when going through with exchanges and enlisting for administrations.

Fig. 3.1 Spying

3.6 Ownership

Ethical discussion has since quite a while ago incorporated the idea of property. This idea has made many conflicts in the realm of cyber ethics. One way of thinking of the web is based on the opportunity of data. The contention over possession happens when the property of data is encroached upon or questionable [16].

3.7 Intellectual property privileges

The consistently speeding up the web and the development of pressure innovation, made the ways for Peer-to-peer document sharing, an innovation that permitted clients to namelessly move records to one another, recently seen on programs. A lot of this, nonetheless, was protected music and unlawful to move to different clients. Regardless of whether it is moral to move protected media is another inquiry. [17].

3.8 Digital gap

An issue explicit to the moral issues of the opportunity of data is the thing that is known as the computerized partition. This alludes to the inconsistent financial split between the individuals who have approached advanced and data innovation, like the internet, and the people who have had restricted or no entrance by any stretch of the imagination. This hole of access between nations or locales of the world is known as the worldwide computerized partition.

3.9 Accessibility, restriction and separating

Accessibility, oversight and sifting raise numerous moral issues that have a few branches in cyber ethics. Many inquiries have emerged which keep on testing our comprehension of protection, security and our interest in the public eye. Over time instruments have been developed for the sake of assurance and security. Web restriction and separating are utilized to control or stifle the distributing or getting to of data [18].

3.10 Freedom of data

Freedom of data, that is the ability to speak freely just as the opportunity to look for, acquire and confer data raises the subject of whom for sure, has the ward in the internet. The right of opportunity of data is usually dependent upon restrictions subject to the nation, society and culture concerned [19].

4. PREVENTIVE MEASURES TO DEAL CYBER CRIME

Because of borderless nature of Cybercrimes, inventive measures are needed to check the issue of various wrongdoings related to sophisticated technology [20-21]. Accordingly, aside from the Cyber Laws, one should remember the accompanying focuses for security in Cyberspace while riding the Internet:

- Mindfulness ought to be produced among the understudies at the grass root level, i.e., information about cybercrimes and digital laws. Digital education ought to be given to the understudies in Computer Centers, Schools, Colleges and Universities too. Digital Law mindfulness program can be coordinated in any instructive organization to give fundamental information on Internet and Internets security.
- Bank and Credit Card proclamations ought to be explored on ordinary premise to lessen the effect of data fraud and violations submitted on the web.
- Usage of proper latest and updated PC will help the computer to remain refreshed. This will lead to a modified security interface which will block the malicious and unauthorized access
- Interesting and solid passwords of eight characters by utilizing a blend of images, words and figures, ought to be saved for online exercises like web based banking. Try not to utilize your email id, login name, and last name, date of birth, month of birth or any such close to home data as your passwords that can be followed without any problem.
- Same passwords ought not to be saved for the web-based assistance used. Save various passwords for various internet based exercises.
- Empower Two-venture Authentication in the webmail to make your webmail or online media account safe from hackers. Add portable number to your mail account so you get told on the off chance that another person attempts to get close enough to your record. Under Two-venture Authentication, your username and secret phrase is needed to open your record.
- For fundamental internet based security, your PC should be ensured by security programming since the product assists with shielding from online dangers. Accordingly, these programming projects are fundamental for remaining protected on the Internet. It incorporates Firewall and Antivirus programs. Firewall controls who and what can speak with your PC on the web. Antivirus additionally keeps up with all internet based exercises, for example, email messages and web perusing and shields the framework from infections, worms, Trojans horse and different kinds of malevolent projects.
- Try not to react to messages that request individual data and don't click on the connections in these messages as they might take you to deceitful and malignant sites. Focus on protection strategy on

Websites and in programming before you share your information with them because authentic organizations don't utilize email messages to request your own data.

CONCLUSION

To close, we can say that the approach in this digital era and recently created advancements have brought about cybercrimes in the couple of years. This has made incredible dangers to humanity on the grounds that the casualty is known to the assailant and he/she with noxious goals like making hurt the PC framework, taking or eradicating information saved in the framework, evolving secret word, hacking charge card subtleties, and ledger number, and so forth, perpetrates such violations. Various sorts of cybercrimes like digital following, digital psychological oppression, digital porn, transforming, imitation, email caricaturing, wholesale fraud, and so forth, have genuine effects over the general public. The cybercriminal gains unapproved admittance to PC assets or some other individual data of the casualty by hacking their record. It is, accordingly, vital for each person to know about these wrongdoings and stay ready and dynamic to keep away from any close to home or expert misfortune.

In any case, to take care of the issue of Cybercrime having worldwide aspects, the public authority of India instituted the Information Technology Act in 2000 to manage such greetings tech wrongdoings. The Act was passed again in 2008 with specific revisions. Eight new offenses were added and the Act was renamed as the Information Technology (Amendment) Act, 2008 alluded to as ITAA, 2008. Aside from this demonstration, certain Sections under the Indian Penal Code (IPC) are likewise utilized as legitimate measures to rebuff the people carrying out such violations. Any misbehavior towards females has been noted as law under the Sexual Harassment of Women at Workplace Act, 2013(Prevention, Prohibition and Redressal). Along these lines, to guarantee equity to the people in question and rebuff the crooks, the legal executive has concocted the above examined enactments.

Everybody should comprehend their responsibilities regarding behaving on the web. A significant part of that is Cyber Ethics. Digital Ethics alludes to the code of capable conduct on the Internet. We should all utilize the fundamental precepts of Cyber Ethics to be responsible cyber citizen.

REFERENCES

[1] Association for Computing Machinery, Inc. Association for Computing Machinery: Code of REFERENCES

[2] Bynum, Terrell Ward. "The Foundation of Computer Ethics," Computers and Society, June 2000,

[3] Cummings, Donavan, Haag, McCubbrey, Pinsonneault, Management Information Systems: For the Information Age, McGraw-Hill Ryerson, 2004

[4] Deborah G. Johnson (2001) Computer Ethics. Prentice Hall.

[5] Esrock, S. L., and Leichty, G. B., 1999, Corporate World Wide Web Pages: Serving the News Media and Other Publics, Journalism &Mass Communication Quarterly 76.3, 456-467.

[6] Gupta, A., Nair, A.P. and Gogula, R., 2003, Corporate governance reporting by Indian companies: a content analysis study, The ICFAI Journal of Corporate Governance, 2.4, 7–18.

[7] SHINDE, S. M. CYBER ETHICS AND LAWS-PROS AND CONS: A STUDY OF IT ACT.

[8] Ramadhan, A., Sensuse, D. I., &Arymurthy, A. M. (2011). E-government ethics: a synergy of computer ethics, information ethics, and cyber ethics. *e-Government*, *2*(8).

[9] Baldini, Gianmarco, Botterman, Maarten, Neisse, Ricardo, and Tallacchini, Mariachiara (2016) “Ethical Design in the Internet of Things,” Science and Engineering Ethics, 1-21.

[10] Rogaway, Philip (2015) “The Moral Character of Cryptographic Work,” http://web.cs.ucdavis.edu/~rogaway/papers/moral.pdf

[11] Cavelty, Myriam D. (2014) “Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities,” Science and Engineering Ethics 20:3, 701-715.

[12] Grodzinsky, Frances S., Miller, Keith W. and Wolf, Marty J. (2012) “Moral responsibility for computing artifacts: “the rules” and issues of trust.” ACM SIGCAS Computers and Society, 42:2, 15-25.

[13] Bynum, Terrell (2011) "Computer and Information Ethics", The Stanford Encyclopedia of Philosophy, Edward N.Zalta(ed.), http://plato.stanford.edu/archives/spr2011/entries/ethics-computer/
[14] Collin, Barry C. "The Future of Cyber Terrorism"Proceedings of 11th annual international symposium on criminal justice Issue. Jemmy, Sprdes&Will, Brars; Examples of Cyber Terrorism.
[15] Hamid, F.Z.A., 2005, Malaysian companies' use of the internet for investor relations,Corporate Governance: The International Journal of Effective Board Performance, 5.1, 5–14.
[16] Healy, P. and Palepu, K., 2001, Information asymmetry, corporate governance disclosure,and the capital markets: a review of the empirical literature, Journal of Accounting and Economics, 31, 405–440.
[17] Hite, R. E., Bellizzi, J. A. and Fraser, C., 1988, A content analysis of ethical policy statements regarding marketing activities. Journal of Business Ethics 7, 771-776.
[18] Ho, P.L., Tower, G. and Barako, D., 2008, Improving governance leads to improved communication, Corporate Ownership and Control, 5.4, 26–33.
[19] Kaptein, M., 2004, Business codes of multinational firms: What do they say? Journal of Business Ethics, 50.1, 13-31.
[20] Verma, D., 2010, 'Web-based business reporting in Indian corporate sector', Journal of Knowledge Management Practice, 11, Special Issue 1,Obtained through the internet: http://www.tlainc.com/articlsi8.htm
[21] Waddock, S. A., Bodwell, C., and Graves, S. B. 2002. Responsibility: The new business imperative. The Academy of Management Executive. 16.2, 132–147.